ABSTRACT

A circuit or software generates a cipher stream. The software models components or the circuit comprises a first and a second plurality of linear feedback shift registers (LFSR). A first of the second plurality of LFSR has a clock signal as a clock input and others of the second plurality of LFSR each have an output of a previous one of the second plurality of LFSR as a clock input. A first of the first plurality of LFSR has the clock signal combined with an output of the first of the second plurality of LFSR as a clock input and others of the first plurality of LFSR each have an output of a previous one of the second plurality of LSFR combined with an output of a previous one of the first plurality of LFSR as a clock input. An output of a last of the first plurality of LFSR and an output of a last of the second plurality of LFSR is combined to produce the cipher stream.